CLAIMS:

1. A method of secure device subscription, wherein
a secret identifier and a public identifier are stored in a subscribing device,
the subscribing device subscribes itself to a subscription authority, involving
a step in which the subscribing device identifies itself with the public identifier, and
a step in which the subscription authority supplies subscription information to the subscribing device,
characterized in that
the method has a first-time subscription protocol and a renewed subscription protocol,
the subscription authority obtains a mapping of the secret identifier during execution of the first-time subscription protocol,
the subscription authority subsequently stores the mapping of the secret identifier, and
the subscription authority uses the stored mapping of the secret identifier during execution of the renewed subscription protocol.

2. The method according to claim 1, wherein during execution of the first-time subscription protocol
the subscription authority and subscribing device commonly and securely obtain a value r,
the subscribing device subsequently encrypts the value r using the secret identifier as encryption key, and
the subscribing device subsequently communicates the encrypted value to the subscription authority.

3. The method according to claim 2, wherein during execution of the first-time subscription protocol
the subscription authority generates the value r, and

the subscription authority communicates the value r securely to the subscribing device.

4. The method according to claim 2, wherein during execution of the first-time subscription protocol the subscription authority and subscribing device commonly generate a value r using a secure common key generation protocol.

5. The method according to claim 2, wherein during execution of any of the subscription protocols

the subscription authority encrypts the subscription information using the value r as encryption key, and

the subscription authority subsequently communicates the encrypted subscription information to the subscribing device.

6. The method according to claim 2, wherein during execution of the renewed subscription protocol the subscription authority communicates the value r encrypted with the secret identifier as encryption key to the subscribing device.

7. The method according to claim 2, wherein the stored mapping of the secret identifier is the value r, encrypted with the secret identifier as encryption key.

8. The method according to claim 7, wherein the value r is also stored by the subscription authority.

9. The method according to claim 1, wherein during execution of the first-time subscription protocol the subscribing device communicates the secret identifier to the subscription authority.

10. The method according to claim 1, wherein during execution of any of the subscription protocols

the subscription authority encrypts the subscription information using the secret identifier, and

the subscription authority subsequently communicates the encrypted subscription information to the subscribing device.

11. The method according to claim 1, wherein the stored mapping of the secret identifier is the secret identifier itself.

12. The method according to claim 1, wherein during execution of the first-time subscription protocol

the subscription authority communicates the subscription information securely to the subscribing device,

the subscribing device subsequently encrypts the subscription information using the secret identifier as encryption key, and

the subscribing device subsequently communicates the encrypted subscription information to the subscription authority.

13. The method according to claim 1, wherein during execution of the renewed subscription protocol the subscription authority communicates the encrypted subscription information to the subscribing device.

14. The method according to claim 1, wherein the stored mapping of the secret identifier is the subscription information encrypted with the secret identifier as encryption key.

15. A subscription authority device for secure device subscription, characterized in that

the subscription authority device is arranged to implement a first-time subscription protocol, during which it receives a mapping of a secret identifier of a subscribing device,

the subscription authority device is arranged to store the mapping of the secret identifier,

the subscription authority device is further arranged to implement a renewed subscription protocol, during which it uses the stored mapping of the secret identifier.

16. A subscribing device to participate in a network requiring subscription, characterized in that

the subscribing device is arranged to contain a public identifier and a secret identifier,

the subscribing device is further arranged to implement a first-time subscription protocol,

during which it transmits a mapping of the secret identifier and during which it receives subscription information,

the subscribing device is further arranged to implement a renewed subscription protocol,

during which it receives subscription information which requires the secret identifier for decryption.

17. A system for secure device subscription, the system comprising
a subscribing device is described in claim 16, and
a subscription authority device is described in claim 15.

18. A signal for secure device subscription, characterized in that the signal carries a mapping of a secret identifier of a subscribing device.

19. The method according to claim 1, wherein a router device that is in connection with the subscribing device acts as the subscription authority.

20. The method according to claim 19, wherein the router device acts as an independent subscription authority.

21. The method according to claim 19, wherein a router device from a group of router devices may act as a virtual single subscription authority.

22. The method according to claim 1, wherein

the subscribing device communicates local data to the subscription authority, and

the subscription authority stores the local data.

23. The method according to claim 22, wherein the subscribing device retrieves at least part of the stored local data from the subscription authority.

24. The method according to claim 1, wherein

the subscribing device encrypts local data using the secret identifier as encryption key,

the subscribing device subsequently communicates the encrypted local data to the subscription authority, and

the subscription authority stores the encrypted local data.

25. The method according to claim 1, wherein

the subscribing device encrypts local data using the secret identifier as encryption key,

the subscribing device subsequently communicates the encrypted local data to the subscription authority, and

the subscription authority decrypts the encrypted local data and stores the decrypted local data.

26. The method according to claim 2, wherein

the subscribing device encrypts local data using the value r as encryption key,

the subscribing device subsequently communicates the encrypted local data to the subscription authority, and

the subscription authority stores the encrypted local data.

27. The method according to claim 2, wherein

the subscribing device encrypts local data using the value r as encryption key,

the subscribing device subsequently communicates the encrypted local data to the subscription authority, and

the subscription authority decrypts the encrypted local data and stores the decrypted local data.